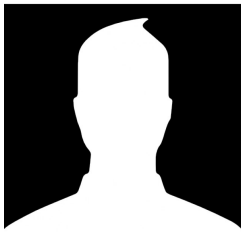
Information Gathering

- Reconnaissance tactics and methods

Håkan Sonesson
hakan.sonesson@atea.se
Senior Security Consultant at Atea

About the speaker

- **Håkan Sonesson**
  - 20 + years experience in information security field.
    - IT-security consultant (Forensics and penetration testing) at IQ AB.
    - CISO at National Courts Administration (Domstolsverket).
    - CISO at Jönköping University (JU).
    - Senior information Security Consultant at Atea (From october 2018).



About the content in this speak

- **Only a snapshot what you can do with information gathering.**
  - Concept and mindset, not a complete overview.
    - See the last slide for more information and sources.

About information gathering

- **Technics and methods to find information about the victim using available sources on internet.**
  - Passive and active information gathering.
    - **Passive** – More or less an attacker anonymous collecting information about the victim using publicly available information (*not from the victims network*).
    - **Active** – Actively collecting information about the victim. For example enumerate relevant information from network services etc.

About information Gathering

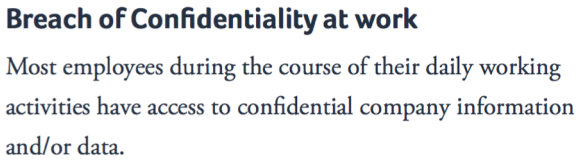
- **Important and powerful step for an attacker.**
  - The more information an attacker manage to gather about the target prior to our attack, the more likely to succeed.
  - Often victims don't understand how much information an attacker can find about an organization and/or person.
    - Small pieces of information could become sensitive together.

About information gathering

- **Why information gathering is powerful for an attacker**
  - "*Give me six hours to chop down a tree and I will spend the first four sharpening the axe*" - (Abraham Lincoln).
  - *"If you know the enemy and know yourself, you need not fear the result of a hundred battles"* - (Sun Tzu).


How Social Media Impacts Data Security

BUSINESS SOLUTIONS Social media is a growing security risk as a source of data leaks and misinformation. Vigilance and training are crucial to minimizing risks for individuals and business.


Breach of Confidentiality at work

Most employees during the course of their daily working activities have access to confidential company information and/or data.


28/03/2018 15:39 BST | **Updated** 28/03/2018 15:39 BST

Google Knows Literally Everything About You

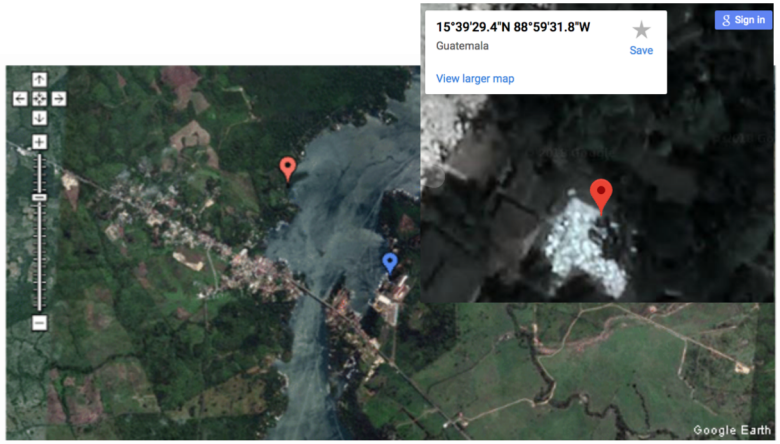
About information gathering

- **Why information gathering is powerful for an attacker**
  - Our footprint on the internet is vast. Even the ”best” slips.

Basic Image Information

Camera:	Apple iPhone 4S
Lens:	4.3 mm
Exposure:	Auto exposure, Program AE, 1/20 sec, f/2.4, ISO 125
Flash:	Off, Did not fire
Date:	**December 3, 2012** 12:26:08PM (timezone not specified) (2 hours, 44 minutes, 59 seconds ago, assuming image timezone of 6 hours behind GMT)
Location:	Latitude/longitude: **15° 39' 29.4" North, 88° 59' 31.8" West** (15.658167, -88.992167) Photos on Jeffrey's blog that are near this location. Map via embedded coordinates at: Google, Yahoo, WikiMapia, OpenStreetMap, Bing (also see the Google Maps pane below) Altitude: 7.152159468 m Timezone guess from earthtools.org: 6 hours behind GMT
File:	**480 × 640** JPEG 132,481 bytes (0.13 megabytes) Image compression: 88% 4% crop of the 3,264 × 2,448 (8.0 megapixel) original
Color Encoding:	WARNING: Color space tagged as sRGB, without an embedded color profile. **Windows and Mac browsers and apps treat the colors randomly.** Images for the web are most widly viewable when in the sRGB color space and with an embedded color profile. See my Introduction to Digital-Image Color Spaces for more information.
Image URL:	http://assets.vice.com/content-images/contentimage/no-flag/[illegible].jpg Apply other tools to this image via ImgOps.com.

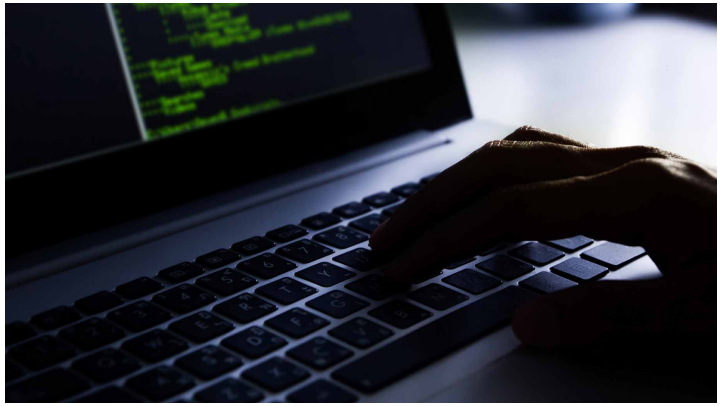
Main image displayed here at 70% width (49% the area of the original)



Fugitive McAfee exposed by basic geotagging feature

Passive information gathering

- **Explore some examples.**



Passive information gathering

- **Scope the victims network**
  - Find IP-range with whois.

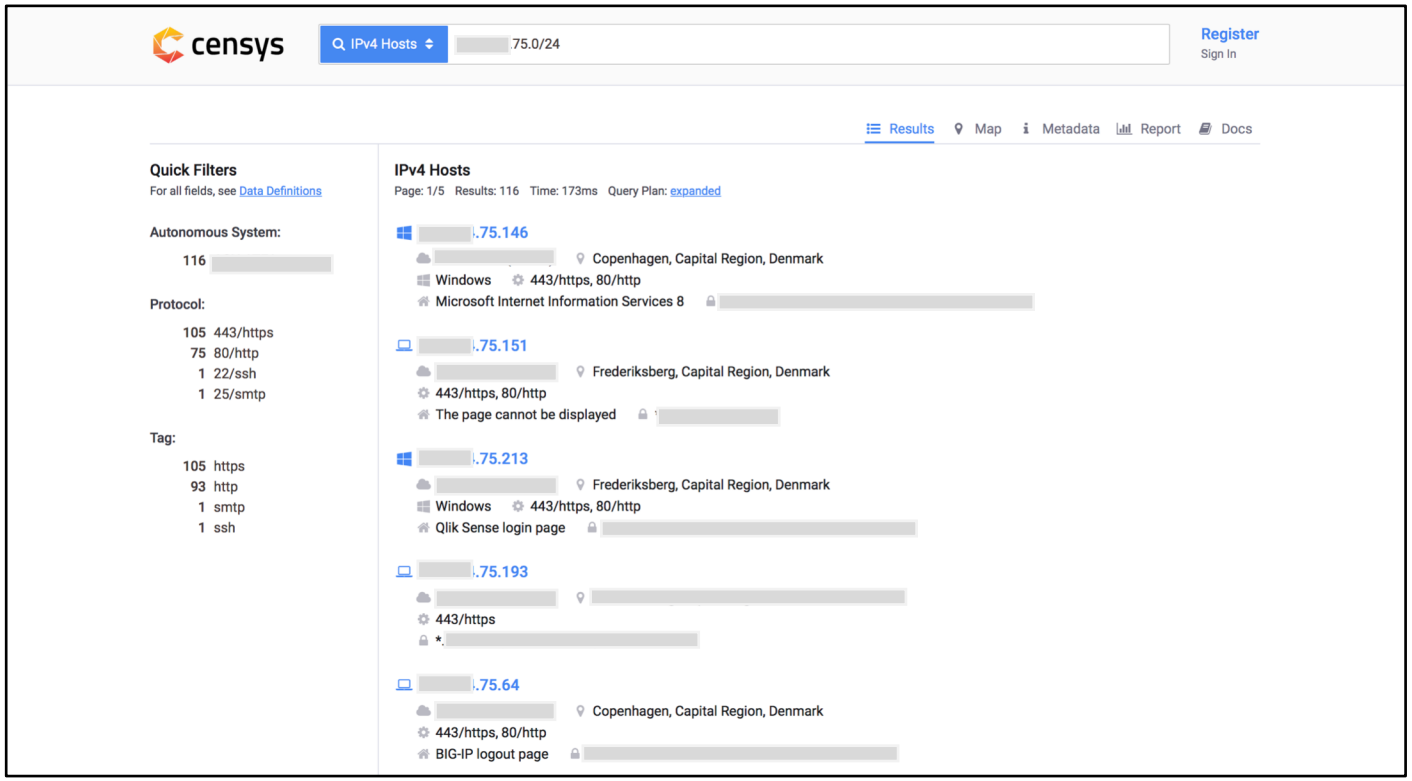
```
root@kali:/# whois -B [redacted].75.240
% This is the RIPE Database query service.
% The objects are in RPSL format.
%
% The RIPE Database is subject to Terms and Conditions.
% See http://www.ripe.net/db/support/db-terms-conditions.pdf

% Information related to '[redacted]72.0 - [redacted].79.255'
```

https://ripe.net

Passive information gathering

- **Scope the victims network**
  - Use censys.io

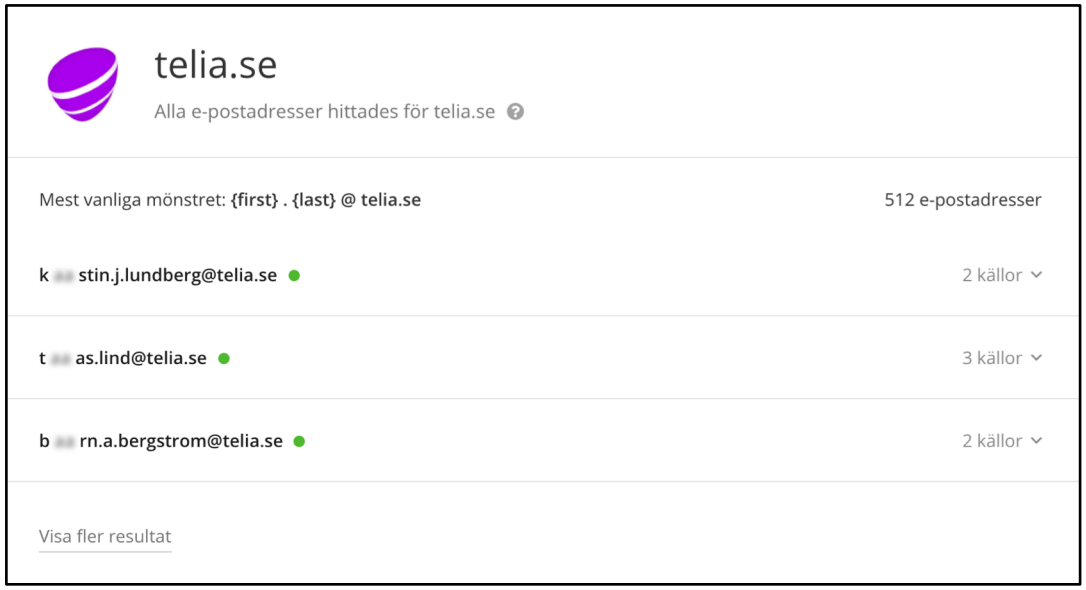


Passive information gathering

- **Scope the victims network**
  - Reverse DNS with theharvester.

Passive information gathering

- **Harvest e-mail**
  - Find e-mail addresses for login or phishing etc.



Passive information gathering

- **Googlebot (spider)**
  - More powerful than people thinks.
    - Diggs deep in organizations web services.
    - Gather words in websites and documents etc.
    - Can disclose sensitive information about the organization.

Passive information gathering

- **Google Hacking**
  - Using Googles search operators to find specific information from an website.
    - Google Hacking Database (GHDB)

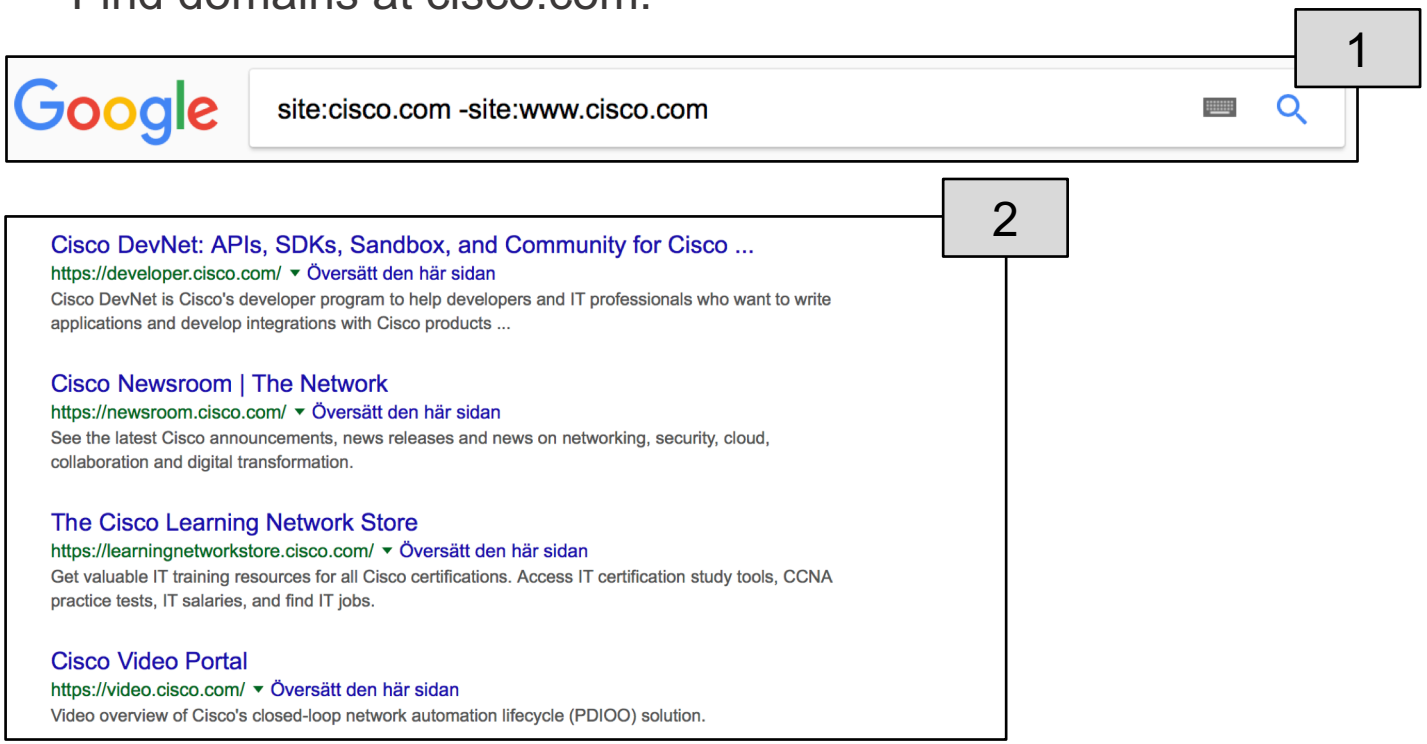
https://www.exploit-db.com

Passive information gathering

- **Google Hacking**
  - Basics
    - `site:<domain.xy>` (**Specific information from the domain**)
    - `ext:<filetype>` (**Information with specific filetype**)
    - `inurl:<string>` (**Websites matches the url-string**)
    - `intext:<string>` (**Websites matches the string**)
    - `intitle:<string>` (**Webtitles matches the string**)
    - `cache:<domain.xy>` (**View a cached copy of the website**)
    - `|` (**Or**)
    - `||` (**And**)

Passive information gathering

- **Google Hacking**
  - Example
    - Find domains at cisco.com.

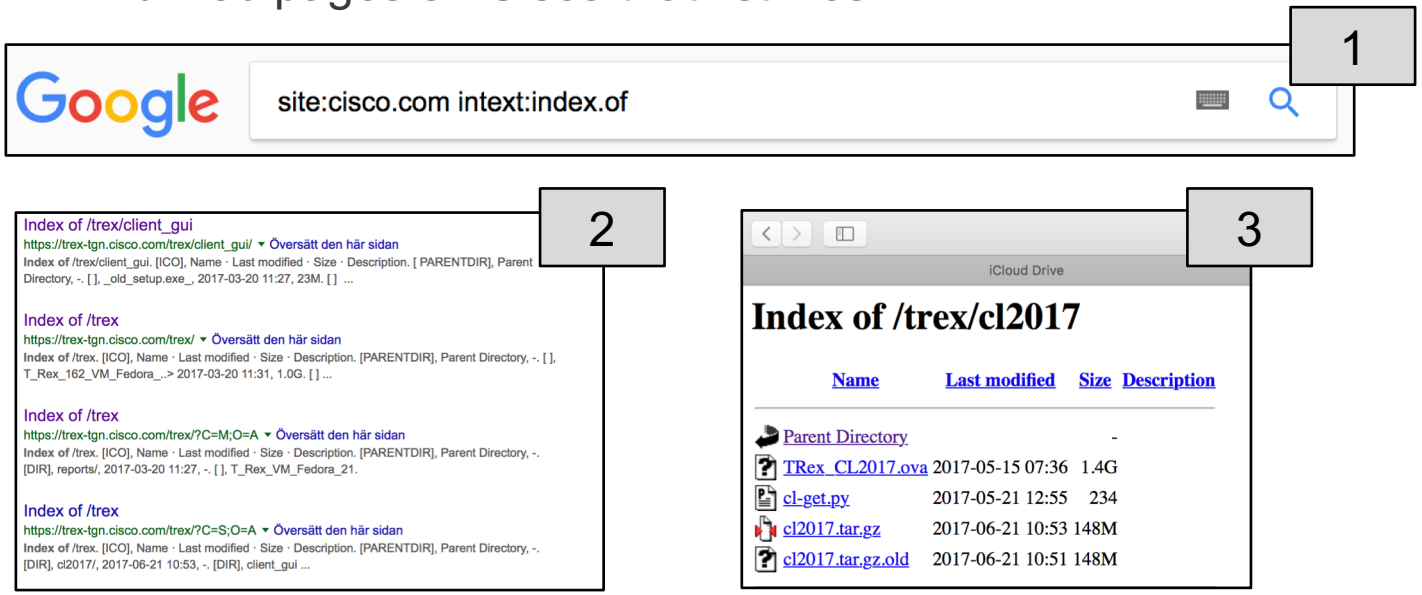


Passive information gathering

- **Google Hacking**
  - Example
    - Find Outlook webaccess service in Sweden.

Passive information gathering

- **Google Hacking**
  - Example
    - Find web pages on Cisco that list files.



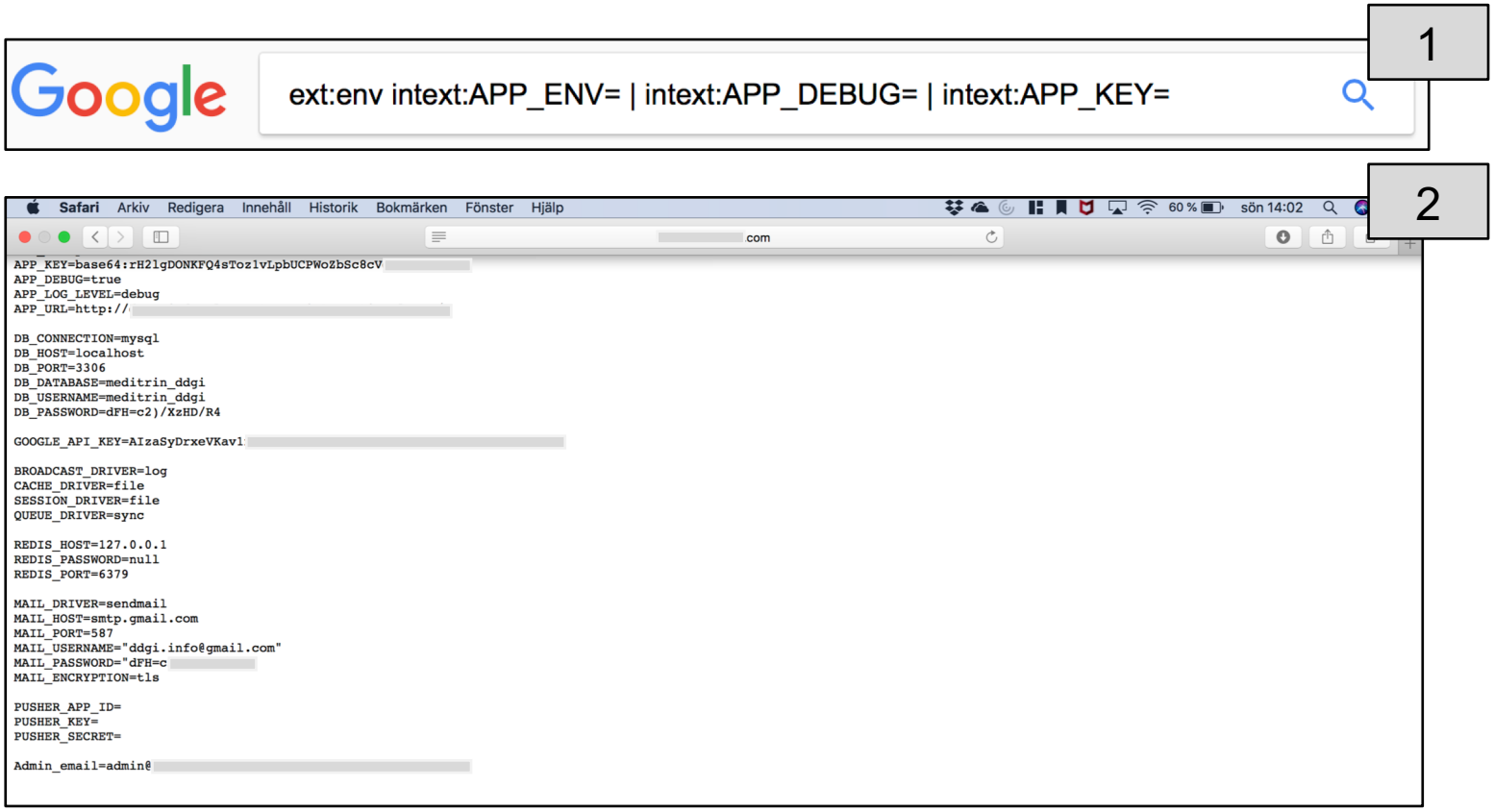
Passive information gathering

- **Google Hacking**
  - Google Dorks, for example find sensitive information.
    - Google Hacking Database (GHDB)

Date	Title	Category
2018-10-26	inurl:phpPgAdmin intext:"Cappuccino" | intext:"Blue/Green"	Various Online Devices
2018-10-25	inurl:filebrowser.wcgp?subDir Communigate	Sensitive Directories
2018-10-24	ext:env intext:APP_ENV= | intext:APP_DEBUG= | intext:APP_KEY=	Files Containing Juicy Info
2018-10-23	inurl:/Portal/Portal.mwsl?PriNav=FileBrowser	Various Online Devices
2018-10-23	inurl:"/wp-json/" -wordpress	Sensitive Directories
2018-10-22	inurl:"/saml2?SAMLRequest="	Pages Containing Login Portals
2018-10-19	inurl:home.tcl intitle:gaia	Various Online Devices
2018-10-17	"[HKEY_CURRENT_USER\Software\SimonTatham\PuTTY\Sessions]" ext:reg	Files Containing Juicy Info
2018-10-17	inurl:"/uddiexplorer/searchpublicregistries.jsp"	Advisories and Vulnerabilities
2018-10-17	inurl="/uddiexplorer/SetupUDDIExplorer.jsp"	Advisories and Vulnerabilities

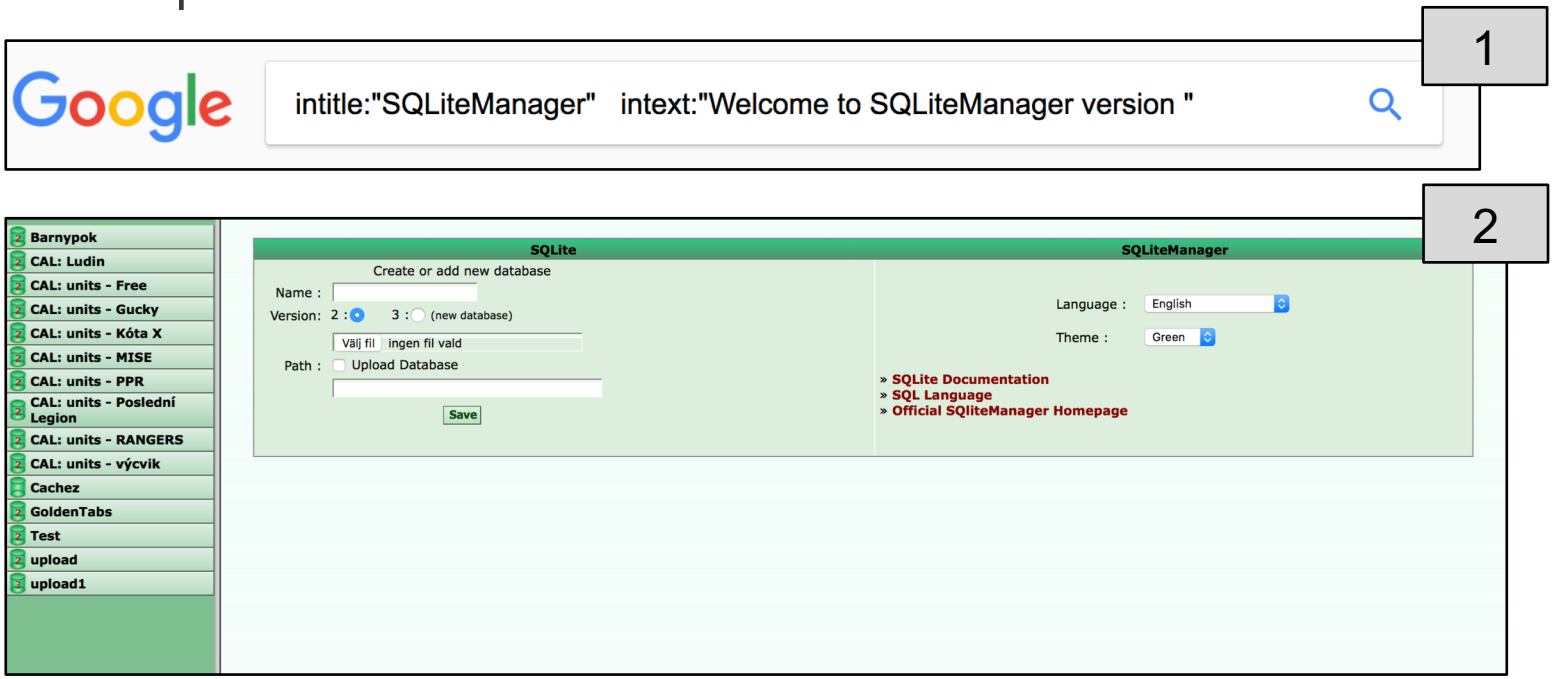
Passive information gathering

- **Google Hacking**
  - Example



Passive information gathering

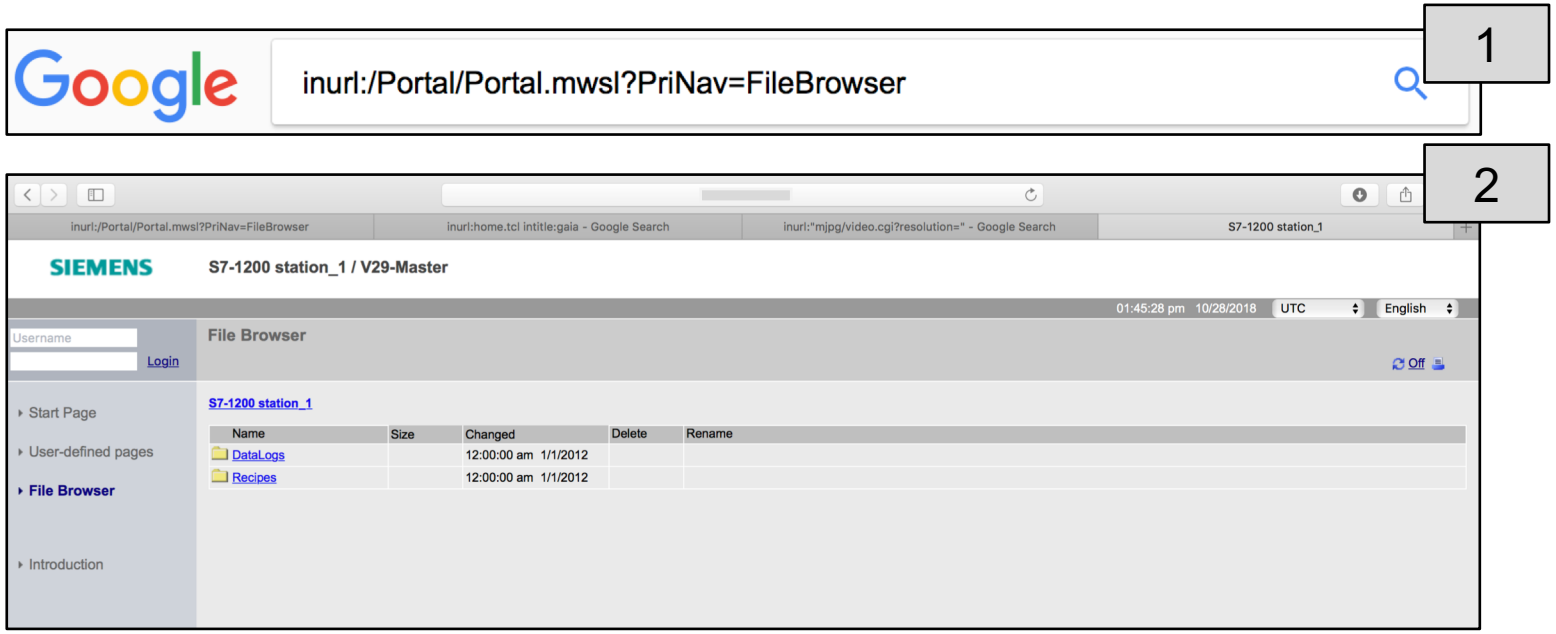
- **Google Hacking**
  - Example



https://www.google.com/search?q=intitle:%22SQLiteManager%22%20+%20intext:%22Welcome%20to%20SQLiteManager%20version%20%22

Passive information gathering

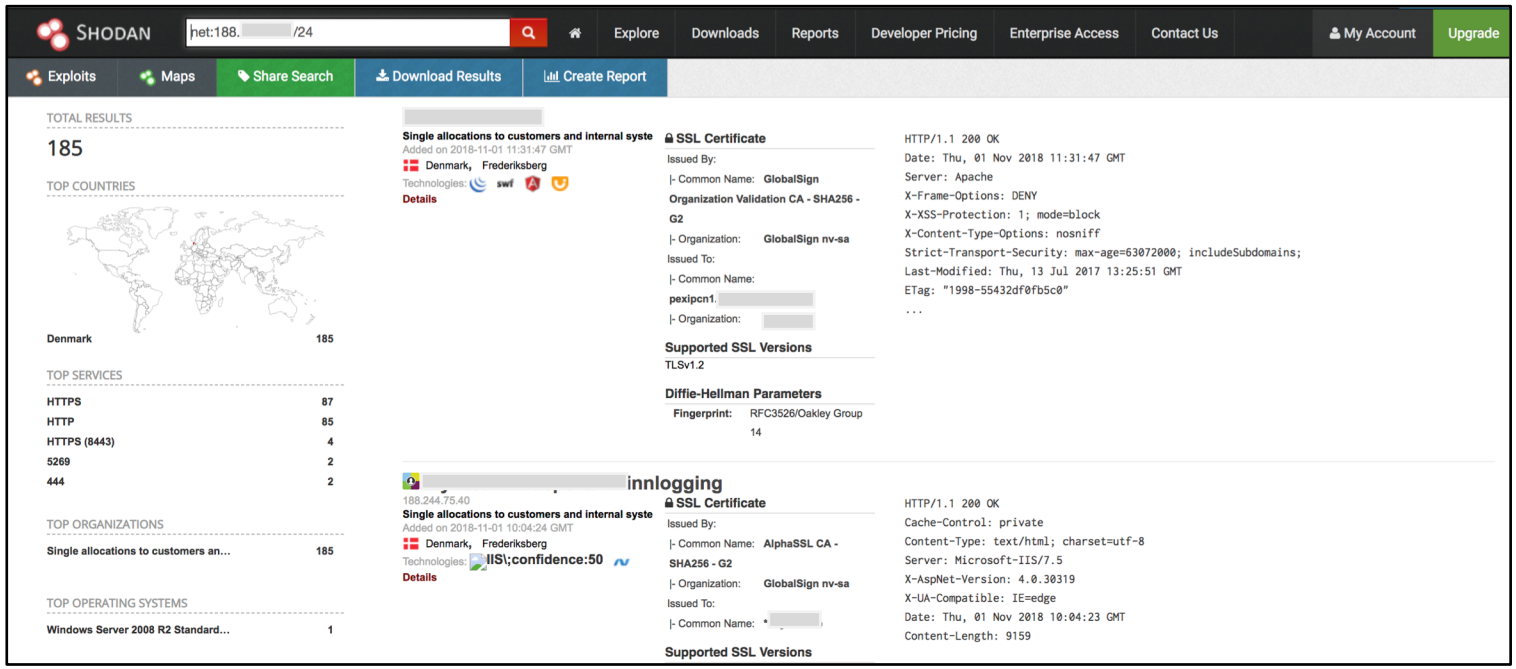
- **Google Hacking**
  - Example



https://www.google.com/search?q=inurl:/Portal/Portal.mwsl?PriNav=FileBrowser

Passive information gathering

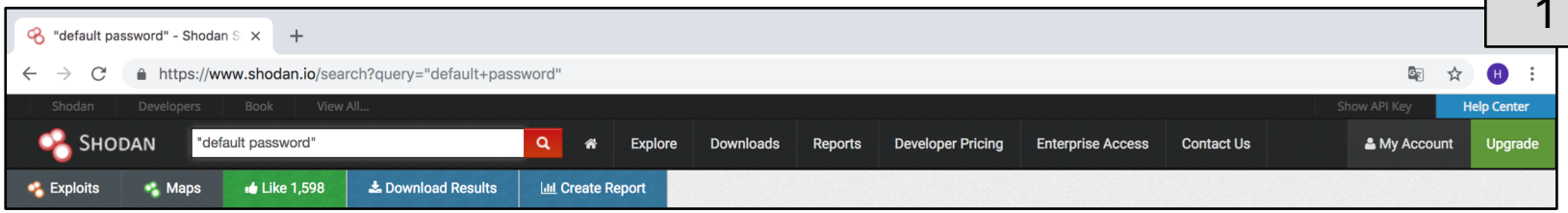
- **Shodan**
  - The search engine for IP-hosts on the internet



Passive information gathering

- **Shodan**
  - Example – Find hosts where banner information show account information.

1

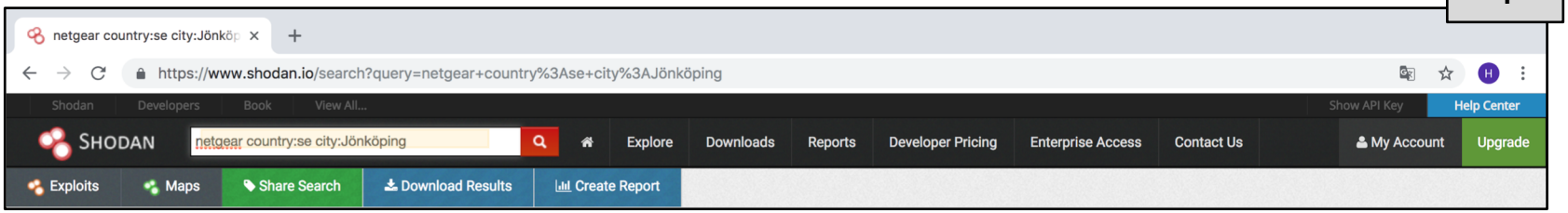


2

Passive information gathering

- **Shodan**
  - Example – Find specific hosts. For example specific city, company etc.

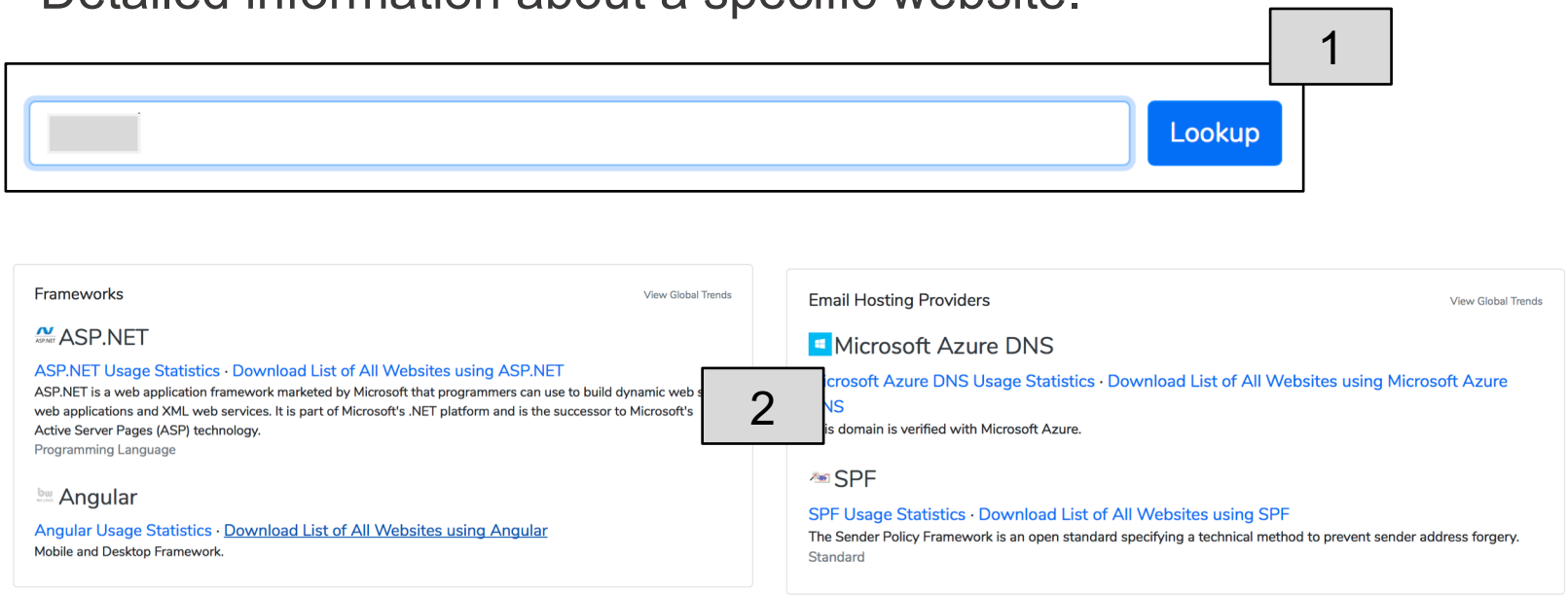
1



2

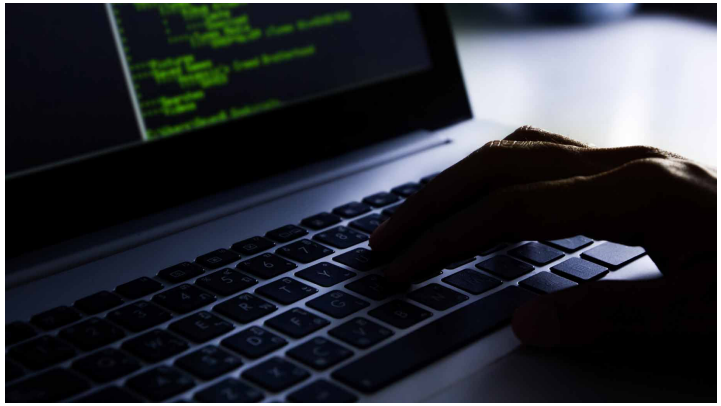
Passive information gathering

- **Builtwith.com**
- Detailed information about a specific website.



Active information gathering

- **Explore some examples.**



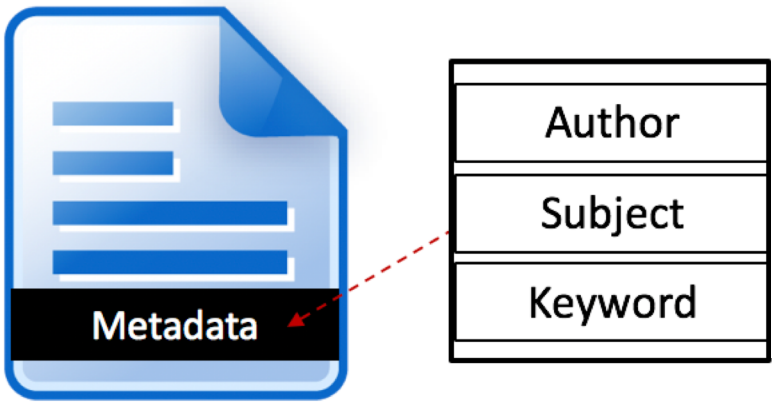
Active information gathering

- **Banner grabbing**
  - Find out what version the service is running.

```
root@kali:~# whatweb [redacted]
http://[redacted]se [301 Moved Permanently] Country[DENMARK][DK], HTTPServer[BigIP], IP[[redacted].75.
240], RedirectLocation[https://www.[redacted]]
https://www.[redacted]se/ [200 OK] Cookies[ARRAffinity], Country[DENMARK][DK], Email[info@[redacted]],
 Frame, HTML5, HttpOnly[ARRAffinity], IP[[redacted]240], JQuery[2.1.1], Open-Graph-Protocol,
Script[text/javascript], Strict-Transport-Security[max-age=15552000], Title[L&#246;sningar, mo
lntj&#228;nster och produkter - Sveriges ledande it-f&#246;retag - Atea], UncommonHeaders[requ
est-context], X-UA-Compatible[IE=edge]
```

Active information gathering

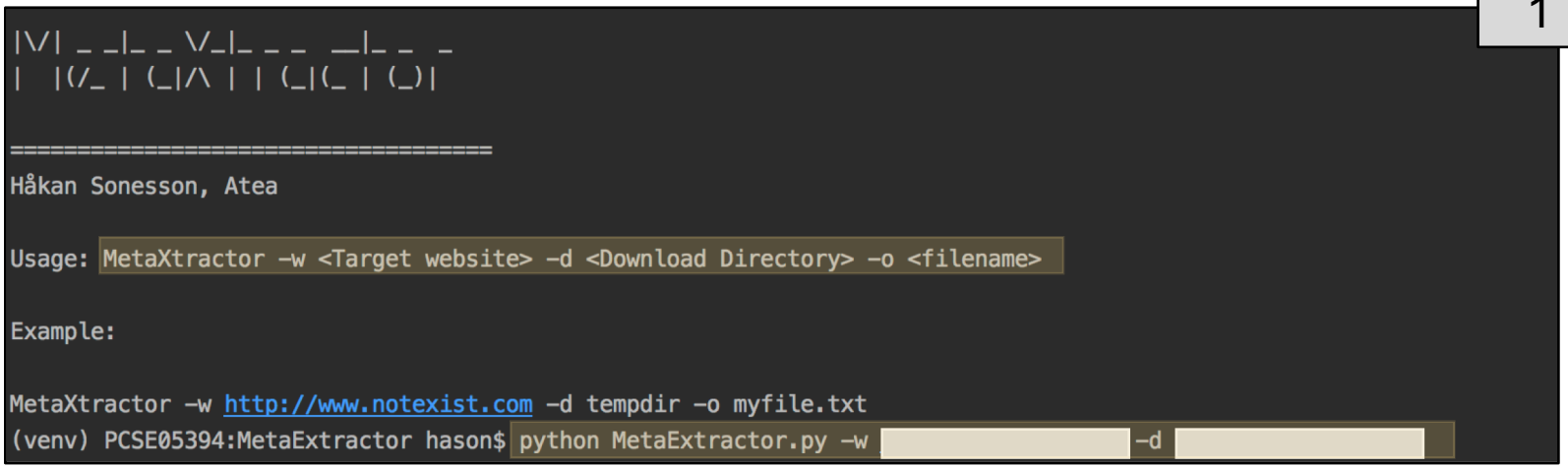
- **Metadata in documents**
  - Saves information about the author, used software, path where the documents is stored etc.
    - Often usernames is saved in the author metadata information.



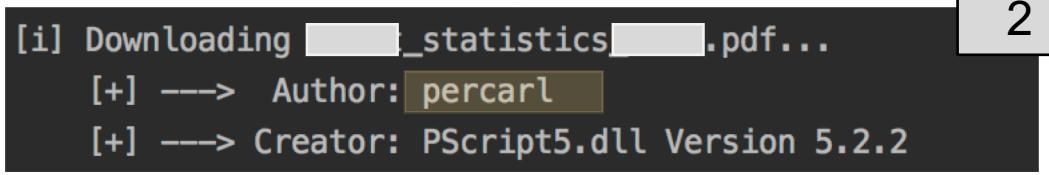
Active information gathering

- **MetadataExtractor (Python-script)**
  - Extract metadata from PDF-files.

1



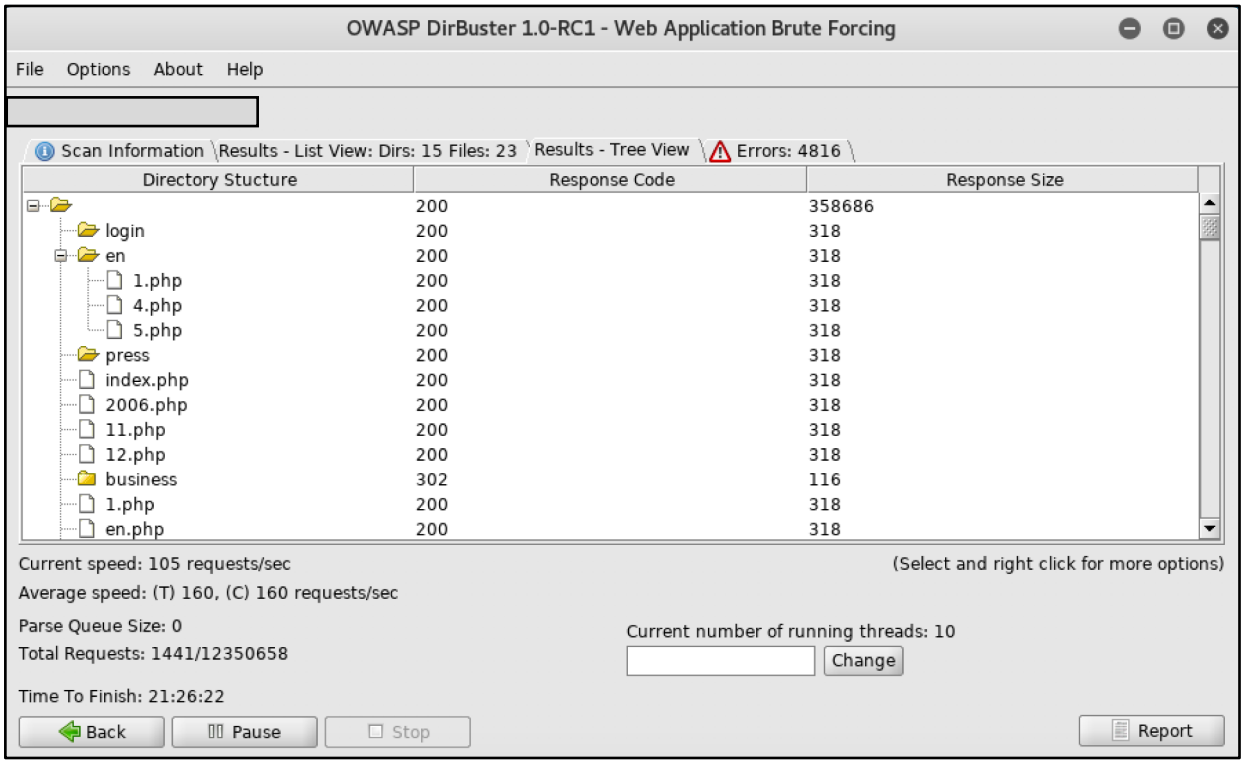
2



https://gist.github.com/SecurityDragon/91f1713f0cae7a384553

Active information gathering

- **Brute force (Directorys and files)**
  - DirBuster (Web Application Brute Force)



Resources

- **Find out more about information gathering.**
  - Tools
    - https://www.spiderfoot.net
    - https://www.elevenpaths.com/labstools/foca/index.html
    - https://www.paterva.com/web7/community/community.php
    - https://www.geocreepy.com
    - https://kali.org
      - The Harvester
      - Recon-ng
      - Maltego (Community)

Resources

- **Find out more about information gathering.**
  - Websites (recourses)
    - https://censys.io
    - https://www.shodan.io
    - https://www.jigsawsecurityenterprise.com
    - https://osintframework.com
    - https://checkusernames.com
    - https://www.exploit-db.com/google-hacking-database/
    - https://builtwith.com
    - https://haveibeenpwned.com
    - https://www.beenverified.com
    - https://www.pipl.com
    - https://www.tineye.com
    - https://www.owasp.org/index.php/Testing:_Information_Gathering